Contents

1. What is Single Sign-On (SSO)? .......................................................................................................................... 3
2. What is Multi-Factor Authentication (MFA)? ..................................................................................................... 3
3. Multi-Factor Authentication Registration/Enrollment (2 Methods Strongly Recommended).................. 3
   i. PingID Smartphone Application (Android and iOS) ...................................................................................... 4
   ii. SMS/Text/Voice Call ......................................................................................................................................... 9
   iii. PingID Desktop App on Windows .................................................................................................................. 12
   iv. YubiKey registration ....................................................................................................................................... 16
4. Manage your devices ........................................................................................................................................... 16
5. Set your primary (default) device ...................................................................................................................... 19

Visit [sso-mfa.dai.com](http://sso-mfa.dai.com) or contact [support@dai.com](mailto:support@dai.com)
1. What is Single Sign-On (SSO)?

Single sign-on (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials. SSO means that you can access all the data and applications you need simply by logging in just once with your DAI username and password.

2. What is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA) is used to ensure that users are who they say they are, while balancing enhanced security with convenience. MFA also provides an extra layer of security when you are accessing DAI systems remotely. Put simply, you’ll have to provide an extra piece of information (for example, a randomly generated number) which—in combination with your username and password—identifies you as authorized to access DAI’s systems. You will not need to use MFA when accessing DAI systems from a DAI corporate or project office, only when you’re working remotely, from home or on the road.

3. Multi-Factor Authentication Registration/Enrollment (2 Methods Strongly Recommended)
   i. To set up your smartphone for MFA, access the following URL from your web browser; https://login.dai.com/PingIDRegistration
   ii. Click on the Register button.
   iii. Log into the application using your windows login credentials (first name initial and last name, e.g. John Silver will use JSilver). Click on Sign On.

Questions? Visit sso-mfa.dai.com or contact support@dai.com
iv. You will be redirected to the following Screen, where you have multiple options to register for MFA (2 methods strongly recommended).

v. If you have already downloaded the PingID App on your smartphone device then click on “I already installed the PingID app”

vi. If you want to use other authentication methods, click on “I want to use a different authentication method”

i. PingID Smartphone Application (Android and iOS)
To set up your smartphone for PingID MFA – complete the following steps to register your smartphone device;

i. Download and install the PingID app using one of the following options:
ii. Android Devices
   a. Open Play Store ( ) on your smartphone and search for PingID (Ping Identity Corporation) and tap Install.
   b. Using the Google Play Store link: On the PingID registration screen, click , and from the Google Play store site, install the app remotely on your Google-registered smartphone.

iii. Apple/iOS Devices
   a. Open App Store on your smartphone, open the iPhone Apps Store ( ) search for PingID (Ping Identity Corporation) and tap Install.
   b. Using the Apple Store link: On the PingID registration screen, click and from the Apple store site, install the app remotely on your iPhone or iPad.

iv. Once the installation of PingID app is complete on your phone, click on “I already installed the PingID app”, you will be redirected to web page with a QR Code and a Pairing Key as displayed below.

v. Open the PingID mobile app on your smartphone, you will be asked to accept the terms of service when you access the PingID mobile app for the first time - Tap Accept.
vi. You will also need to enable push notifications and location for PingID. Accept all PingID permission requests when prompted (tap Allow and OK).

vii. PingID app will be ready to scan the QR code to complete the pairing process, point your smartphone device at the QR code on the registration page.

a. If you are unable to scan the QR code, on your smartphone tap Enter Pairing Key Manually and enter the pairing key as shown on the registration page.

viii. Once the QR code has been scanned or Pairing Key has been entered, you will see a green checkmark indicating pairing has been successful, you will be redirected to Complete Your Profile page automatically.

ix. Enter a nickname for your profile –DAI, optionally add a picture, and then tap Done.
x. After completing the registration, you will see the PingID app screen with a one-time passcode number and your organization name in the organization list.

xi. An authentication request is generated immediately. To complete the pairing process, authenticate using your smartphone by swiping the ID button up.
xii. Once you are authenticated, you will see a green checkmark confirming successful authentication.

xiii. Once registration is completed you will see below screen.
ii. **SMS/Text/Voice Call**

To set up SMS or Voice authentication, you need to pair your device with your account. Pairing a device creates a trust between your device and your account, so you can use your device to authenticate during the login process.

Once you have paired your device, each time you log in to your account, or application, you will receive a one-time passcode (OTP) via SMS/Text or voice call with which to authenticate.

**Set up SMS or Voice Call authentication**

i. Log into the application using your active directory credentials. Click on Sign On.

ii. The PingID registration page is displayed. Click on **“I want to use a different authentication method”**.
iii. Alternative Authentication pop-up screen will appear on your screen.

![Alternative Authentication](image)

Authentication Preference
To verify your identity with one-time passcodes, select your authentication preference.

- Receive passcodes via SMS
- Receive passcodes via voice call
- Authenticate with YubiKey
- Authenticate using the desktop application

Next

iv. In the Alternative Authentication popup window:
   a. Enter your authentication preference (select either Receive passcodes via SMS or Receive passcodes via Voice Call).
   b. Select the country code via the dropdown list, enter your phone number and then click Next.

![Alternative Authentication](image)

Questions?
Visit [sso-mfa.dai.com](http://sso-mfa.dai.com) or contact [support@dai.com](mailto:support@dai.com)
v. Enter the passcode into the **Authentication** screen field, and then click **Verify**.

![Authentication screen](image)

vi. When successfully verified, you'll see the green checkmark authenticated sign and will be redirected to your account or app.

![Authenticated sign](image)

vii. Next time when you try to log in to your organization dock, or application, a One Time Passcode (OTP) will be sent to your mobile phone and you will be prompted to enter it in your browser. Enter the OTP in the Authentication window in your browser and click **Sign On** to complete the authentication.

![Authentication window](image)

Questions? Visit [sso-mfa.dai.com](https://sso-mfa.dai.com) or contact [support@dai.com](mailto:support@dai.com)
iii. **PingID Desktop App on Windows**

PingID enables you to sign in to all your applications with the added security of multifactor authentication. Use the PingID desktop app to generate a One-Time Passcode from your computer that you can use to authenticate.

Set up desktop authentication on Windows

i. Login to your account or app. The PingID registration page is displayed. Click **I want to use a different authentication method**.

![PingID desktop app](image)

ii. In the **Alternative Authentication popup** window, select **Authenticate using the desktop application** and click **Next**.

![Alternative Authentication](image)

iii. In the Desktop Setup window, you'll see the pairing key that you'll need later.

Visit [sso-mfa.dai.com](http://sso-mfa.dai.com) or contact [support@dai.com](mailto:support@dai.com)
iv. Click Download for Windows and save the file to your local drive.

v. Click the pingID.exe download file to launch the Desktop installer and if prompted ‘do you want to allow this app to make changes to your PC?’ click Yes. The PingID Setup wizard will open.

vi. Review the Software License Agreement, click “I accept the agreement”, and then click Next. The files are extracted and PingID for desktop app will be installed and launched.
vii. Enter the pairing key you were given earlier and click Pair.

![PingID pairing key input](image1)

viii. You will need to create a 6-digit PIN for your desktop application.

![PingID create PIN](image2)

ix. The desktop app generates a passcode and then launches the Authenticating window in a browser.

Visit [sso-mfa.dai.com](http://sso-mfa.dai.com) or contact [support@dai.com](mailto:support@dai.com)
x. In the desktop app, click Copy to copy the passcode, paste it into the Authentication field in your browser and then click Sign On.

xi. You'll see the green checkmark indicating authentication is successful, and your browser is redirected to the dock or app you wanted to access.

Visit sso-mfa.dai.com or contact support@dai.com
xii. Next time you want to log in to the PingID dock or an application, launch the PingID desktop app and enter your PIN to generate a passcode, and enter the passcode when prompted during the log in process.

iv. **YubiKey registration**

   i. Insert the YubiKey into your machine’s USB port for quick pairing of device

   ![YubiKey Insertion](image.png)

   NOTE: You can use any of the multifactor method during the login.

4. **Manage your devices**

   You can add, remove or edit the devices that you use for authentication. If you have more than one device paired with your account, you can select an alternative device to authenticate with during the login process.

   i. Once logged in, click on your name on the top right corner and then click on Devices.

   ![My Devices](image.png)

   ii. Click on +Add.
iii. Click on SMS. Select the appropriate country and enter your phone number. Click Next.

iv. Enter the six-digit verification code received as a SMS/Text and click on Verify.

v. Click on Add again.

Visit sso-mfa.dai.com or contact support@dai.com
vi. Click on Voice. Select the appropriate country and enter your phone number. Click Next.

![Voice selection screen](image)

vii. Enter the verification code from the call and click on Verify.

![Verification code entry screen](image)

viii. Click on Add again.
5. Set your primary (default) device

Default to primary: You select a primary device on your Devices page. Each time you log on, you are prompted to authenticate using your primary device. The log in page provides the option to change devices and select a different device with which you wish to authenticate during the authentication process.

The Devices page shows the devices you currently have paired with your account. The primary device is shown in green. You can switch between the Authenticating Devices by selecting the preferred method as shown below:

After the second factor verification, user will be allowed to his application via his dashboard:

Visit sso-mfa.dai.com or contact support@dai.com
Visit sso-mfa.dai.com or contact support@dai.com